I thought to write short comment

1. Cybersecurity rule amendment is a good first baby step that SEC.gov is taking. As a career engineer, cybersecurity professional – (though now I am so burnt. And I find cybersecurity field dreadful, full of apathy); I like that…though entire new division at SEC.gov for handling cybersecurity would be necessary and required EVENTUALLY. It is the mindset of management – as I have already replied to SEC.gov twitter handle about this rulemaking – a separate DIVISION – more professionals at SEC handling, auditing, enforcing cybersecurity would be needed. And as I asked that "are you creating a separate division for this?"

2. Frank Abagnale, the infamous impostor turned security advisor, said

   "Every breach, without exception, happens because somebody in that company did something they weren't supposed to do or somebody failed to do something they were supposed to do—didn't fix its tech, it didn't update patches, so the hackers got millions of pieces of data."

3. **Like SOX internal controls and audit that came out** – after ENRON – similar to what I experienced at GE….**cybersecurity internal controls implementation and audit is a MUST.**. SEC has not done/ proposed any rulemaking in this regard; and hope that it will be done in the future, we can only hope…

4. **SEC prosed rule does not specifically state how company should report ZERO day vulnerability – rulemaking says "Incident" – does zero day vulnerability mean "Incident that is Material in terms of SEC's definition of reporting" ?** – which could be result of poorly done product/service, self-inflicted misery , company having SLACKER type approach, serious defect in code, design, deployment, system that has led to finding of zero day vulnerability by someone else….when company issues public patch about zero day vulnerability (as well as CISA, NIST cybersecurity alerts as mentioned below)--- it would be better to put that in SEC filing – so stake holders – those who I believe read SEC regulatory filings – would be better informed.

5. **SEC rule amendment states that "Specifically, we are proposing amendments to require current reporting about material cybersecurity incidents."**

   Does it mean that company's CISA, NIST and CVE cybersecurity alerts are MATERIAL INCIDENTS and should/MUST be reported as part of this amendment?

   There is not much clarity on what is MATERIAL, and it is likely that it will be subjective ..

May be SEC can specifically mention that any alerts issued through CISA.gov, NIST, CVE – with score above this –MUST be reported to SEC. Because this is a PROACTIVE step….in a long run – investors would be educated about how many alerts company is issuing and of what Severity, how much bad things are, how quickly company is ISSUING PUBLIC ALERT after coming to know about it, how management is handling it…this is a way to address risk, liability and damage to public, patient, investor , employee data, systems, and more—entire universe that cybersecurity touches –OR say anything connected on internet.

SEC rule amendment states that "Disclosure of Cybersecurity Incidents that Have Become Material in the Aggregate" – which is more than welcome. Punishes serial offender and forces them to disclose. And company's approach to fix issues in PRODUCTION, worry later and benefit now because we are in hurry to (1) go to market(2) in hurry to capture market share (3)we don't want to spend money initially (4) just slacker approach and mindset (5) who cares – thinking that "no one is going to jail "– worst –will pay some fine someday if at all, if regulatory agency comes after –but in the mean time we have generated 10-50 times revenue, profit, captured market share and more – that comparatively "paying a fine- which would be 1-5 % at the MOST of the amount revenue was generated, profit, captured market share and time to go to market….and this is all calculated by management as I have seen first-hand – managers think this way and do this way– so -- ☺

6. **SEC Rule for internal whistleblower –** proposed rulemaking does not mention anything about it.
   In 2020, when SEC amended SEC rule 21F-2 to incorporate supreme court ruling in Digital realty v. Somers ; and removed protection for internal reporting ---two commissioners (Ms. Lee and Ms. Crenshaw) voted against it, where commissioner quoted history of whistleblower dated back to 1776 ; what founding father of America did back then (entire history is that because of the whistleblower reporting- naval commander had to leave his post ---) –I had submitted comments for rule making; but voting was 3-2 by commissioners and then SEC chairman Jay Clayton(who voted against it- though I had emailed at commissioners and chairman, general counsel email address about not to remove it)- -

   Since SEC is already amending rule –and based on my detailed phone conversation with SEC.GOV senior attorney – SEC has to follow what supreme court ruled about in Digital Realty v. Somers case **as definition of whistleblower**–

meaning those who report to SEC ONLY and not internal whistleblower. Currently two bills in house and senate are pending since 2019; those bills amend current whistleblower definition and add those who report internally as well. So there is some congressional intent. It is likely that– congress people knows about my lawsuit (I have already mentioned those bills in my lawsuit filing in 2019)..and GE has lots of lobbying power – so these two bills are sitting idle since 2019….

So coming back to my discussion….this is a good way to make SEC rule for cybersecurity more effective by adding internal reporting protection.

7. **Currently there is NOT any SPECIFIC statute or rule - specific to cybersecurity whistleblowing and/or reporting.** Most of the time employee would report to management - internally and try to fix it / address it.
8. **SEC rule amendment about Board skill and expertise is really a great step** – in my case – I had right from beginning emailed GE board of director about security issues at GE healthcare and ; she had replied that she was as a board member of GE- too high to deal with individual complaint….but then from next SEC.GOV filings – it shows that that same board of director was assigned cybersecurity oversight at GE..and she had a BIOLOGY background.

GE 2019 proxy statement – page 17
BOARD SKILLS AND EXPERIENCE

Technology Experience
As a digital industrial company

9. **Proactively changing culture where speaking up of** - bring up cybersecurity vulnerability is not a SIN - and without fear of retaliation. Those employee who DISCLSOE cybersecurity vulnerabilities, VERY FIRS, and INSTANTLY get a status of Persona non grata ; because disclosing in PUBLIC vulnerability means exposing – weakness
10. Changing culture of cybersecurity, proactively addressing issue throughout product, software, system LIFE CYCLE DEVELOPMENT- “starting form functional requirement, product requirement specification to design, development, testing, deployment and maintenance “ - would require lots of cultural changes, changes in funding, management mindset, not to be overconfident, be realistic, not to cut corners, and also status quo , --- all these can be achieved by putting back old SEC rule 21F-2 ‘s internal reporting whistleblower protection and not that only those who report to SEC are protected under Dodd Frank act…
11. **GE removed in SEC 10-K and /or DEF 14 A**

So GE REMOVED/STOPPED putting BELOW SECTION entirely from February 24, 2019 till present 2022 in SEC 10-K filing with securities & exchange commission; after Trivedi sent email - on January 2019 to Culp, GE board of directors **about Remote connectivity-**and wrote that Trivedi would be filing a lawsuit against GE..... **and GE has since REMOVED that section from SEC 10-k altogether…..**

----------SEC.gov website; searching GE's public filing with SEC
Filing 10-K - For year 2007, 2008, 2009, 2010, 2011, 2012, 2013, 2014, 2015, 2016, 2017 mentions INSITEEXC as follow

Item 7 operations..SIGNIFICANT TRENDS & DEVELOPMENTS MD&A

Healthcare SEGMENT - Our product services include remote diagnostic and repair services for medical equipment manufactured by GE and by others, as well as computerized data management and customer productivity services.
OR
Healthcare systems also offers product services that include remote diagnostic and repair services for medical equipment manufactured by GE and by others.

12. **For example – GE added word "CYBERSECURITY" in its SEC.GOV filings after my fight…**

- ✓ **2011 DEF 14- A proxy statement**
  https://www.sec.gov/Archives/edgar/data/0000040545/000119312511065578/ddef14a.htm

- ✓ **2012 DEF 14- schedule 14 A -proxy statement**
  https://www.sec.gov/Archives/edgar/data/0000040545/000119312512107087/d301131ddef14a.htm

- ✓ **2013 DEF 14-A– there is no mention of WORD "CYBERSECURITY"**
  https://www.sec.gov/Archives/edgar/data/40545/000120677413001019/ge_def14a.htm

- ✓ **2014 DEF 14- A proxy statement – filed on** 2014-03-05 , reporting for 2014-04-23 ; **WORD "CYBERSECURITY"**
  Is mentioned once under experience of Dan Heintzelman.
  https://www.sec.gov/Archives/edgar/data/0000040545/000120677414000746/ge_def14a.htm

  Trivedi did private arbitration with GE in May 2014(in a hotel room)—and Trivedi spoke with FBI agent couple of weeks prior to arbitration hearing(where FBI supervisor said that what GE was doing is called QUITAM =- fraud against government)

- ✓ **2015 DEF 14 A**
  https://www.sec.gov/Archives/edgar/data/0000040545/000120677415000847/ge_def14a.htm

  WORD "CYBERSECURITY" is mentioned 7 times in 2015 DEF 14A
  Also mentions on page 12- "CHANGES MADE IN RESPONSE TO 2014 EVALUATIONS. In response to feedback received from our directors in 2014, the Board determined to adjust the compositions of the Audit Committee and Risk Committee in light of the increased demands on both of these committees and formalize and strengthen the Audit Committee's oversight responsibility for cybersecurity."

13. Data breach of employees' personally identifiable information, third party liability
    - ✓ **SEC proposed rules states that "iii) The registrant has policies and procedures to oversee and identify the cybersecurity risks associated with its use of any third party service provider, including, but not limited to, those providers that have access to the registrant's customer and employee data."**
    - ✓ **This is to the point – and I liked it too.**
    - ✓ **In re GE/CBPS DATA BREACH LITIGATION (1:20-cv-02903-KPF) District Court, S.D. New York**

      https://www.courthousenews.com/author/courthouse-news-staff/

      Corporate negligence Brief / August 4, 2021

NEW YORK — A federal judge ruled that General Electric employees may sue Canon and GE after a data breach at the imaging company resulted in the release of **GE employees' personally identifiable information**. GE's policy documents may be read as implied contracts that gave its employees reason to believe it would **protect employees' personal information, including information provided to third party vendors.**

- ✓ On February 21, 2022 GE reached a settlement for this class action lawsuit. Atleast one judge was doing her job. Judge ruled that

"[T]he Supreme Court has made clear that 'allegations of possible future injury' or even an 'objectively reasonable likelihood' of future injury are insufficient to confer standing." McMorris, 995 F.3d at 300 (quoting Clapper v. Amnesty Int'l USA, 568 U.S. 398, 409-10 (2013)). Rather, a future injury may support standing only if "the threatened injury is certainly impending, or there is a substantial risk that the harm will occur." Id. (quoting Susan B. Anthony List v. Driehaus, 573 U.S. 149, 158 (2014)).

- ✓ Judge Katherine Polk Failla's order denying GE's motion to dismiss – dated August 4, 2021. **In this ruling--- "at risk " ,"future injury" has been shown enough to prove injury and thus ARTICLE III standing...**

14. GE or a COMPANY's MINDSET on CYBERSECURITY as shown in an example below---remote connectivity is better than defects (below is GE architect Bill Barbiaux deposition; which has been part of my lawsuit filings)

Q So your -- I'm talking about -- I'm just consolidating everything in one sentence. Your point was connectivity is better than defects in Insite ExC. At the least we would have connectivity?
A Right.
Q And some are unresolved for ten years, which

is, as you said, not acceptable. But given that there was no alternative, it went on?
A Right. And like I said, it was purchased software, so I don't know that any of these were really ten years old because we weren't even in production at that point, but they may be.

15. At GE healthcare, as GE architect testified in his deposition – that the remote connectivity platform failed all security tests on DAY1 – on a public facing web; so GE Healthcare – moved connectivity platform INSIDE GE's network- INTRANET. And choose not to fix any of the cybersecurity vulnerabilities – for those tests failed on DAY 1 and kept using the platform for several years…while old and new vulnerabilities were PILING up in terms of hundreds of critical design defects(in terms of FDA- Food and Drug administration's language it is called "Design nonconformance and critical defects) and vulnerabilities.

Shouldn't there be some rule from SEC around this…to fix this kind of behavior and also force company to disclose such defects in cybersecurity.
FDA has **21CFR820 QUALITY SYSTEM REGULATION Subpart I--Nonconforming Product – but FDA is known to be administrative agency and not good at enforcing ..so ….my point is SEC should amend rule making for cybersecurity – non confirming product….**

16. This is the IOT internet of things event I did.

IoT Security: High Stakes for Billions of Devices
https://vlab.org/events/iot-security-high-stake-billions-devices/
"The speed of Internet of Things (IoT) adoption is creating opportunities for startups developing IoT security solutions. Many industries such as healthcare, energy, automotive, and consumer products are being transformed using insights gained from the real-time data that IoT provides. As new online devices continue to be added at exponential rates, the frequency of sophisticated cyber attacks targeting consumers, businesses, and public services is also increasing.
Startups are competing against large corporations to establish themselves as leaders in IoT security. And the rewards leading the charge to protect against security breaches, hijacking, and individual privacy concerns is enormous. According to KBV Research, the IoT Security market expected to reach $29.2B by 2022.

- Is the Internet of Things making us more vulnerable to attacks?
- Given the anticipated growth in connected devices, will security solutions be able to keep pace?

- What are the biggest challenges for startups working on IoT Security? ‘

17. As SEC staff and top brass knows about my matter that I have sued GE , GE Healthcare. *Trivedi v. Gen. Elec. Co.*, CV 19-11862-PBS, District of Massacusetts and currently pending at first circuit – Trivedi v. General Electric et. al - No. 21-1434. Though judicary and judges are also corrupt.
18. As we all know GE has changed its marketing, PR and entire company profile as “GE is a digital industrial company” -- and all of its SEC.GOV regulatory filings also reflect that; while in reality – GE had stoneage cybersecurity practice – and Also in SEC.gov filings dated 2013 till date; it shows that GE painted ROSY picture , look trendy and cool--of it’s digital solutions (Internet of Things platform);
As stated in SEC 8-K form; that **“it’s market is up to $8 billion and wants everybody using it”** …

- but GE totally failed to consider RISKS, liability –even that putting many GE assets – where some GE assets are age OLD, due to several limitations of computing processing power, processing memory available; unable to get cyber security patches and upgrades due to these reasons..
- This is misleading given that GE has lessons to be learned at the same time was recklessly, negligently connecting all kinds of assets on internet.

19. **Also SEC should include disclosure of annual training of staff and management. There must be mandatory training that company reports it undertook for its employees.**
20. Below is Cybersecurity related CISA.gov alerts…these are portion of **ALERTS** related to **healthcare and REMOTE CONNECTIVITY–** but complete list is available on cisa.gov. **My point to mention it here -- is that SEC proposed rulemaking to INCLUDE such cybersecurity alerts through CISA, NIST ; and over period of time – aggregate of such alerts, how it MATERIALLY impacted customers, users, patients, employees, society – how company handled it, when it was reported and when it became public –when PATCH was released, when recall was done…These alerts are Material information. But current rulemaking language is not clear about it.**

Some catalog of cybersecurity vulnerabilities alert GE issues through CISA - department of homeland security – there is long list on cisa.gov.

Item 1 is holy grail -Scott Erven – cybersecurity researcher reported first to GE about it in 2014- as it affect 100s of 1000s of medical devices- specifically and exactly

what GE is touting in all their SEC filings as robust (and it also involves InsiteEXC remote connectivity platform – the one that Trivedi is fighting for), with lack of internal controls and more. And GE knew it ; but nor GE or DHS, cared to issue alert for 4 years– and randomly – issued alert on Feb. 2018. Since 2014 – there was a lot of press and media coverage about Scott Erven's finding. At that time, GE shrugged off and didn't give a damn. Scott Erven himself ahs been surprised about this kind of inaction by GE..

So my point is -- SEC rulemaking should include – clause where company is required to issue cybersecurity alert – no matter what – regardless of looking bad, being exposed, tarnishing of company's image and what not --- by certain time limit – and not wait for 4 years – currently this part is in VACCUM – no specific mention about it in proposed rule.

Latest in December 2020, GE is issuing alert through DHS for remote connectivity issues—
So as SEC proposed rule suggest – previous undisclosed incidents in aggregate to be reported and disclosed as material…It shows a pattern.

1. **Advisory (ICSMA-18-037-02) GE Medical Devices Vulnerability** Original release date: March 13, 2018

https://us-cert.cisa.gov/ics/advisories/ICSMA-18-037-02

2. **ICS Medical Advisory (ICSMA-19-190-01)** GE Aestiva and Aespire Anesthesia (Update A)release date: July 09, 2019 |

https://us-cert.cisa.gov/ics/advisories/icsma-19-190-01

3. **ICS Advisory (ICSMA-20-023-01) GE CARESCAPE,** ApexPro, and Clinical Information Center systems release date: January 23, 2020

https://us-cert.cisa.gov/ics/advisories/icsma-20-023-01

4. **ICS Medical Advisory (ICSMA-20-343-01) GE Healthcare Imaging** and Ultrasound Products Original release date: December 08, 2020

https://us-cert.cisa.gov/ics/advisories/icsma-20-343-01

5. **ICS Medical Advisory (ICSMA-20-049-02)** GE Ultrasound products Original release date: February 18, 2020

https://us-cert.cisa.gov/ics/advisories/icsma-20-049-02

6. **ICS Advisory** (ICSMA-18-128-01) Silex Technology SX-500/SD-320AN or GE Healthcare MobileLink (Update B) release date: May 08, 2018

7. ICS Advisory (ICSA-18-275-02) GE Communicator release date: October 02, 20181

https://us-cert.cisa.gov/ics/advisories/ICSA-18-275-02

Note:- I see that people are having meeting / video conference with commissioner (s) and SEC staff. I would like to have one with Commissioner Lee and Crenshaw as well as David Joire. But I don't know how to request setting up this meeting. So kindly reply me in email soon about how to set up this meeting. Deadline is approaching – so we can still set up a quick video conference. Thanks.

Madhuri Trivedi

- Twitter - @madhuritrivd
- Linkedin:- linkedin.com/in/trivedim
- World innovation and Entrepreneurship – THE WSIE summit speaker invite– Great presenter 2019 - https://thewsie.com/presenters-2019/
- **Here's my cybersecurity whistleblower profile on whistleblowers.org**

https://www.whistleblowers.org/whistleblowers/madhuri-trivedi/